DEFEATING 802.11 WIRELESS NETWORKS

GRADUATE RESEARCH PAPER

Charles R. Cosnowski, Major, USAF

AFIT/ICW/ENG/08-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this graduate research project are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/ICW/ENG/08-01

DEFEATING 802.11 WIRELESS NETWORKS

GRADUATE RESEARCH PAPER

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

Charles R. Cosnowski, BS, MAS, MS

Major, USAF

June 2008

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

AFIT/ICW/ENG/08-01

DEFEATING 802.11 WIRELESS NETWORKS

Charles R. Cosnowski, BS, MAS, MS

Major, USAF

Approved:

____________________________________ ________

Dr. Robert F. Mills (Chairman) Date

____________________________________ ________

Mr. Timothy H. Lacey (Member) Date

AFIT/ICW/ENG/08-01

Abstract

Homeland security of the United States is constantly under threat of attack from terrorist organizations. A viable and current terrorist threat is the use of unmanned aerial vehicles (UAVs) as weapons of mass destruction. These UAVs can be built simply and cheaply from commercial off the shelf (COTS) parts and are typically controlled using standard radio control (RC) technology. An emerging technology that is being implemented to control and communicate with UAVs is the 802.11 wireless network protocol or Wi-Fi.

This project discusses various portions of the Wi-Fi protocol and analyzes the protocol to determine techniques for first detecting and then defeating wireless networks utilizing the protocol through denial or deception. The first set of techniques presented defeats a network through denial. These denial techniques are divided into two categories: broad area denial techniques and specific network denial techniques. After denial techniques are discussed a process for deceiving an 802.11 wireless network is presented.

AFIT/ICW/ENG/08-01

To my beautiful wife, my boys and moje Polskie dziecki (my Polish children) for their love, support, laughter, motivation and life purpose they have given me.

Acknowledgements

I would like to express my sincere appreciation to all those that helped make my year at AFIT a successful and memorable experience. I cannot thank my graduate research paper advisor, Dr. Robert Mills, enough for his countless hours of guidance, thought-provoking questions, and constant vectoring throughout my writing of this paper. I would also like to thank Dr. Barry Mullins for his excellent classroom instruction which provided me the knowledge foundation to pursue this project.

Charles R. Cosnowski

Table of Contents

Page

List of Figures

Figure Page

List of Tables

Table Page

AFIT/ENG/08J

DEFEATING 802.11 WIRELESS NETWORKS

I. Introduction

Background

On a cold crisp October night in Detroit, Michigan, Comerica Park is packed with 42,000 fans as the Tigers are nearing victory over the St. Louis Cardinals in game five of the World Series. The crowd is completely unaware of the approaching danger as several small unmanned aerial vehicles (UAVs) are launched from surrounding parks and fields. With just over a mile to go to their target, and with speeds over 80mph, the 4 UAVs are at the edge of the stadium within 75 seconds after launch. The first of the UAVs clips a light post as it dives into the stadium and scatters parts over the crowd. The Cardinals dugout however, takes a direct hit with the second plane exploding about 10 feet above the ground and scattering a fine white dust over the players, coaches and staff. Another UAV flies north towards the main upper deck and dispenses the same white cloud of dust as it explodes halfway up the stands. The last UAV misses the stadium altogether and crashes directly into Interstate 75, just north of the ballpark.

Nobody is seriously injured in the attacks, but the ensuing panic results in 17 deaths and over 100 injured as the fans trample one another attempting to flee the stadium. That evening, the associated press (AP) is inundated with emails from the East Turkestan Islamic Movement (ETIM) claiming responsibility and threatening a similar attack in two days at game six in St. Louis unless all Uyghur detainees are released from captivity at Guantanamo. The powder dispensed by the UAVs is found to be innocuous, but ETIM promises to deliver a true biological/chemical attack if their demands are not met.

Although the events that occur in this scenario are fictitious, they represent a viable and current threat. Using common off the shelf (COTS) parts terrorist organizations have the willingness and capability to produce UAVs, like the ones used in the scenario, as effective weapons of terror or worse, as weapons of mass destruction.

Black Dart

To analyze this threat, the Defense Intelligence Agency (DIA) organized the first Black Dart project in 2003. Black Dart is an annual exercise held at China Lake Naval Air Weapons Station which investigates the threat of UAVs and also the capabilities to counter the UAV threat. In 2005, a team consisting of members from the Air Force Research Laboratory (AFRL) and Aeronautical Systems Center (ASC) participated in Black Dart III (BD III) (AFRL and ASC 2005:2).

The primary objective of BD III was to assess the threat of an adversary's ability to design and construct a system that could attack a specific object or person on the ground using a small UAV built from COTS parts. The threat that the AFRL/ASC team decided upon for BD III consisted of multiple identical "cruise missile" type vehicles where the vehicles themselves were the weapons as opposed to delivering a separate weapon. The mission profiles of the strategy that the team used consisted of three phases; launch, cruise, and terminal (AFRL and ASC 2005:6-7).

In the launch phase, multiple UAVs would be launched in a coordinated attack most likely from a single launch site. A single launch was decided to be the best plan of action since the footprint was smaller and the chances of being discovered prior to launch were decreased. A single launch site also has the advantage of selecting from multiple different sites to take advantage of weather factors, such as winds, or to avoid areas that may have unanticipated increased security. During the cruise and terminal phases of the flight profile, the UAVs are flown actively to their target, passively/autonomously using an onboard integrated INS/GPS, or a combination of both techniques to provide guidance to the target area. Guidance during the cruise phase can be fairly inaccurate to achieve the objectives of the phase. However, during the terminal phase of the attack, more precision would be required to ensure that the vehicle is flown to the precise desired location. The best way to achieve this precision is through the use of video signals sent from the vehicle. These video signals provide the pilot of the vehicle a first person view of the craft's flight path (AFRL and ASC 2005:13-15).

Currently most COTS parts and accessories for radio controlled (RC) aircraft utilize basic radio frequency (RF) signals set to one frequency to control the aircraft and to receive video signals from any onboard cameras. The aircraft receives control inputs from a transmitter on a single frequency using either Pulse Position Modulation (PPM), which sends signals to the aircraft based on the length of time the transmitter is on during a certain time slot, or Pulse Code Modulation (PCM), which uses binary codes to control the aircraft. These systems are susceptible to interference from other signals generated on the same frequency and are limited in range due to line of sight. Some newer RC aircraft are using spread spectrum technology to send signals to the aircraft. This technology encodes the signal being sent from the transmitter to the aircraft so that the signal is largely indiscernible from other noise in the same frequency band. Although spread spectrum decreases the chances of interference to almost zero, line of sight between the transmitter and receiver is still required.

In the not so distant future, controlling and receiving video signals from a commercially built RC aircraft will not be limited by line of sight. RC aircraft of the future will have the ability to be controlled and communicate via wireless network infrastructures that exist today. The purpose of this paper is to discuss techniques to defeat or disrupt wireless data streams of the 802.11 wireless network architecture. The 802.11 wireless network protocol was chosen since this architecture has a longer range capability than other architectures, such as 802.15 (Bluetooth), and is currently the most more widely used wireless network protocol. Although the UAV threat was the motivation for this project, the techniques presented in this project can be used to defeat any 802.11 wireless network.

Chapter 2 provides an overview of the most widely used wireless network architecture being used today; 802.11 (Wi-Fi). This overview will discuss how data is transmitted to and from users, security measures that can be implemented in the architecture, and lastly the structure of the data frames that are used in the protocol. Chapter 3 will define steps to take in order to defeat an 802.11 wireless network. These steps will discuss various techniques for defeating a wireless network through denial and deception. Lastly, chapter 4 will conclude the project with a summary.

II. Literature Review

Internet Access

There are basically three ways a user can access the internet from home or work. The first and earliest way is through dial-up access. This type of access is usually very slow since it utilizes standard telephone lines which are limited in their capacity to carry digital information. Typically users who still access the internet through a dial-up connection have no other way to connect to the information super highway. The next way to access the internet is through a broadband connection. Examples include Digital Subscriber Line (DSL) or a cable modem. Although faster than dial-up, this type of access is still limited by requiring the user to use a physical cable to connect to the network. The last and most recent addition to the internet access options is a wireless connection. With this type of access a user can connect from nearly any location as long as they are within the signal range of a wireless access point. Within this access type there are three standards that users and devices can use to communicate with each other and the internet.

The first of these standards is the Institute of Electrical and Electronics Engineers (IEEE) 802.15 standard or more commonly known as Bluetooth. Bluetooth operates over a short range, at low power, and at a low cost. This type of network is sometimes referred to as a wireless personal area network, (WPAN) due to its very short range. The second wireless network standard is the IEEE 802.11 standard or more commonly known as Wi-Fi. Wi-Fi provides greater distances, typically a couple hundred feet, or perhaps miles when using directional antennas (Kurose 2007:544). With these greater distances Wi-Fi is typically used in conjunction with local area networks (LAN). The final wireless network standard is the IEEE 802.16 standard which is more commonly known as WiMAX. WiMAX provides even greater distances than Wi-Fi with the capability to provide internet access to users within 3000 square miles of a WiMAX access point (Grabinowski, undated).

The two wireless standards that have the capability to provide signals to a mobile user or device over great distances are Wi-Fi and WiMAX. However, WiMAX is a fairly new system and is not highly proliferated. This next section will provide an overview of the Wi-Fi protocol. The majority of the information in this next section was taken from the book *Computer Networking: A Top-Down Approach*, by James F. Kurose and Keith W. Ross.

Wi-Fi Standards

In the early 90s, there were many wireless LAN technologies and standards being developed. The winner that emerged from this battle was the 802.11 Wi-Fi standard. There are many 802.11 standards that are in use today, with the most prevalent being 802.11b, 802.11a, and 802.11g. The difference between these standards is shown in Table 1. 802.11b has a data rate of only 11 Mbps and operates in the unlicensed 2.4 GHz band and competes with other devices in this band such as cord less phones and microwave ovens. 802.11a achieves a higher bit rate but in a higher frequency band. This higher frequency decreases the transmission distance of the signal. The 802.11g standard operates in the lower frequency band while providing the higher bit rate offered by 802.11a (Kurose, 2007:527).

Table 1. Summary of IEEE 802.11 Standards

Standard	US Freq. Range	Data Rate
802.11b	2.4-2.485 GHz	Up to 11 Mbps
802.11a	5.1-5.8 GHz	Up to 54 Mbps
802.11g	2.4-2.485 GHz	Up to 54 Mbps

Wi-Fi Architecture

The basic building block of the 802.11 architecture is called the basic service set (BSS). Central to a BSS is the base station, also known as an access point (AP). The AP is typically connected via a network cable to a router which is then connected to the internet. Wireless stations are also a fundamental part of the BSS. These wireless stations are typically the end-user devices that connect to the AP, such as a personal digital assistant (PDA) or a laptop computer. Just like in a wired LAN, each wireless station interface has an associated 6-byte Medium Access Control (MAC) address as well as the interface for the AP (Kurose, 2007:527). Figure 1 shows a typical 802.11 architecture.

The architecture shown in Figure 1 is typically referred to as an infrastructure wireless LAN. The infrastructure is the APs and the wired internet structure associated with this network. Typically wireless infrastructure LANs are limited to a couple BSS that can cover the area of a large building such as an airport or a university. However, some cities in the United States, such as Philadelphia, are undergoing ambitious plans to have one large LAN cover an entire metropolitan area. The project in Philadelphia,

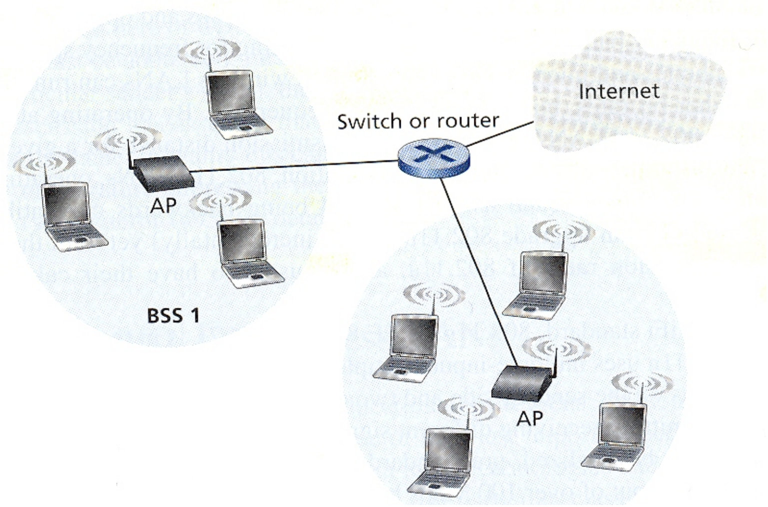


Figure 1. Wi-Fi Architecture (Kurose, 2007:528)

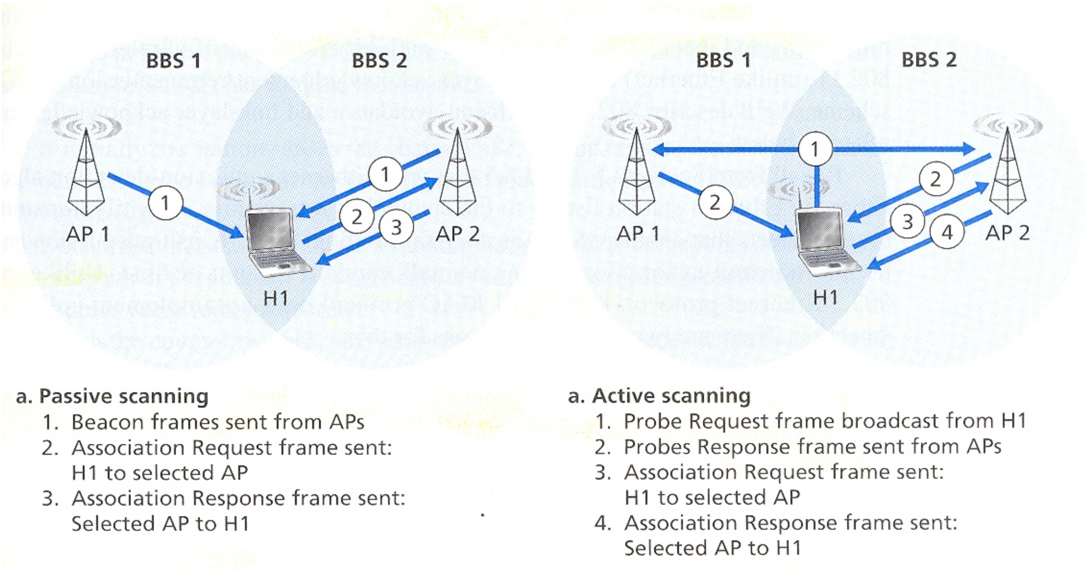
called Wireless Philadelphia, plans to cover over 135 square miles (Merritt, 2005). The BSS of a wireless LAN can also be extended out over a great distance using directional antennas. During the DEFCON Wi-Fi Shootout 2005, a team of amateur radio operators successfully established an unamplified 802.11b link over a distance of 124.9 miles. This link required large antennas on both ends of the link and also required line of sight between the two antennas, but proved that unamplified 802.11 signals can be sent over long distances using directional antennas (Keeney, undated).

Wi-Fi wireless stations also have the capability to connect directly to one another and exchange data in what is called an ad-hoc network. An ad-hoc network has no central AP and with no wireless connections to the larger internet (Kurose, 2007:527). Due to the limited range of ad-hoc networks, the Wi-Fi discussion will focus on the 802.11 infrastructure mode.

Connecting to an AP

Before a wireless station can send or receive any network data, the station first needs to associate with an AP. When an AP is initially setup, a Service Set Identifier

(SSID) and frequency is assigned to the AP. In the 802.11 standards that operate in the 2.4 GHz to 2.485 GHz range, there are 11 overlapping channels. Channels are non-overlapping when they are separated by four or more channels. The only set of three non-overlapping channels are 1, 6, and 11 (Kurose, 2007:529). The 802.11 standard requires that an AP send out beacon frames periodically. These beacon frames include the AP's SSID and MAC address. A wireless station listens over all 11 channels for these beacon frames that are being broadcasted. Typically, if a wireless station is set to automatically connect to any AP, the station will attempt to connect to the AP that has the strongest signal. The wireless station then transmits an association request frame to the AP. The AP then responds with an association response frame. This process of listening for beacon frames and associating is also called passive scanning. In active scanning, the wireless station broadcasts a probe frame that is received by all the APs within the range of the wireless station. The APs then respond to the wireless station with a probe response frame. Then the wireless station decides which responding AP to associate with. Figure 2 provides a graphical representation of passive and active scanning. After the wireless station is associated with an AP, the station will attempt to join the subnet of the AP. This is typically done using the dynamic host configuration protocol (DHCP) (Kurose, 2007:530). During the association process, the wireless station may be required to authenticate itself to the AP. There are many approaches to authentication, such as permitting access based on the wireless station's MAC address or requiring the use of usernames and passwords. A more in depth discussion of authentication techniques will be discussed in the Wi-Fi security section.



a. Passive scanning
1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: Selected AP to H1

a. Active scanning
1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent: Selected AP to H1

Figure 2. Wireless Station Active and Passive Scanning (Kurose, 2007:531)

Wi-Fi MAC Protocol

After a wireless station is associated with an AP and has successfully joined the subnet of the AP, the station can then start sending and receiving data frames to the AP. However, like with a wired medium such as Ethernet, multiple wireless stations (or even other APs) may be attempting to send and receive data to the same AP. This dilemma requires a multiple access protocol. The 802.11 standard follows the precedent set by Ethernet and uses a random access protocol. For Wi-Fi, this protocol is called carrier sense multiple access (CSMA). The term carrier sense means that each wireless station senses the channel before transmitting and subsequently avoids transmitting when the channel is sensed busy. Although both Ethernet and 802.11 use CSMA, Ethernet uses collision detection (CSMA/CD) techniques where as 802.11 uses collision avoidance techniques (CSMA/CA) (Kurose, 2007:532).

There are two main reasons that 802.11 uses collision avoidance rather than collision detection like Ethernet. The first reason is that the ability to detect collisions requires the transmitting node to send and receive at the same time. Typically, received signals are much weaker than transmitted signals. To be able to detect a received signal while transmitting would require a wireless card to have one antenna for transmitting and another for receiving. This would be cost prohibitive. The second reason, and most importantly, is that even if the wireless card could transmit and receive at the same time, there is still no assurance that the card would be able to detect all collisions, due to a situation called the hidden terminal problem (Kurose, 2007:532). The hidden terminal problem is when two or more wireless stations associated with an AP can transmit and receive data to the AP, but are too far apart from each other to detect the other station's signals. Figure 3 gives an example of the hidden terminal problem.

In Figure 3, the wireless stations located at H1 and H2 are associated with the AP located in the middle and have no problem sending and receiving signals from the AP.

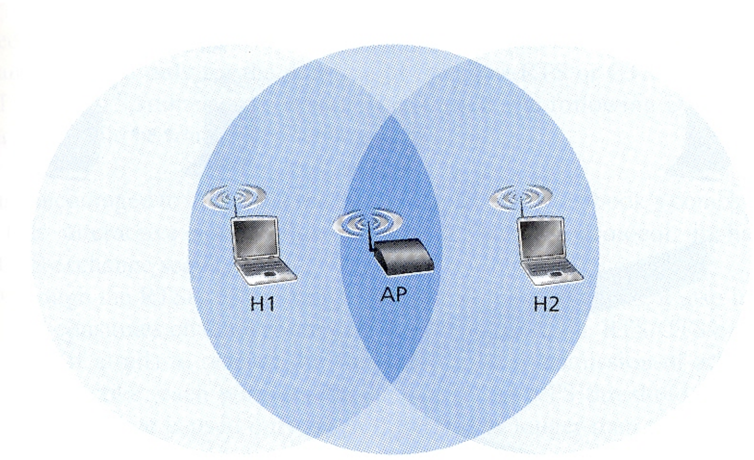


Figure 3. Hidden Terminal Problem (Kurose, 2007:535)

However, the two wireless stations are unable to receive signals transmitted by the other wireless station.

Since the 802.11 multiple access protocol of CSMA/CA does not use collision detection, the wireless station will transmit the entire data frame once it starts transmitting. Due to the high bit error rates associated with a wireless channel, 802.11 also uses a link-layer acknowledgement scheme. When the AP receives a frame that passes the cyclic redundancy check, the AP then waits a small amount of time and then sends back an acknowledgement frame. This wait time is known as the Short Inter-frame Spacing (SIFS). If the wireless station that transmitted the frame does not receive the acknowledgement from the AP within a specified amount of time, the wireless station assumes that an error occurred and retransmits the entire frame again, using the CSMA/CA protocol. If the wireless station does not receive the acknowledgement frame from the AP after a set number of retransmissions, the transmitting station gives up and discards the frame (Kurose, 2007:533).

Now that the Wi-Fi link-layer acknowledgement scheme has been explained, the CSMA/CA protocol can be discussed. The following scenario presents the steps that are taken when a wireless station or AP (a node) attempts to transmit a frame to another AP:

1. The node first senses the channel to determine if it is idle or busy.
2. If the channel is idle, the node transmits the entire frame after waiting a specified amount of time called the Distributed Inter-frame Space (DIFS).

3. If the channel is sensed busy, the node backs off and waits for a random amount of time. This waiting time starts once the channel is sensed idle and freezes when the channel is sensed busy.

4. Once the wait time expires, which can only occur when the channel is idle, the node then transmits the entire frame and then waits for the acknowledgement frame.

5. If an acknowledgement is received, the node knows that the frame was correctly received by the AP. The node transmits the next frame, if required, starting at step 3 of the protocol. Without an acknowledgement, the node goes to step 3 as well, but with a longer interval (Kurose, 2007:534). Figure 4 shows an example of the 802.11 link-layer acknowledgment scheme.

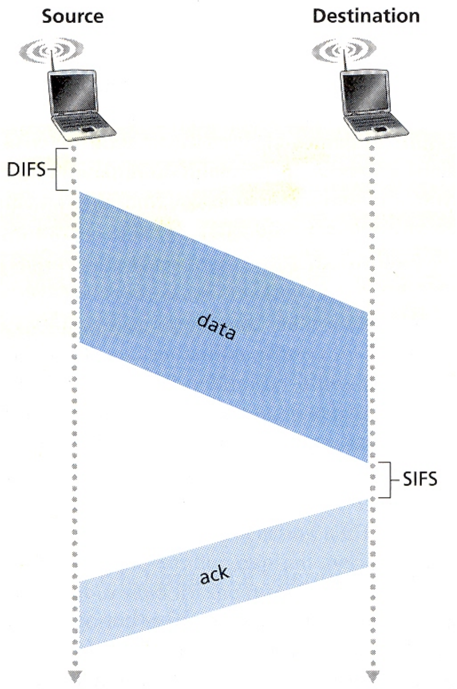


Figure 4. 802.11 Link-Layer Acknowledgements (Kurose, 2007:533)

From these steps one can see how the 802.11 CSMA/CA protocol avoids collisions, rather than detecting them. For example, if two nodes want to transmit a frame but they sense that the channel is busy, they both wait a random amount of time before transmitting. Statistically, the random wait times should be different. When the channel becomes idle, the node with the shorter wait time will begin transmitting. The other node will sense that the first node is transmitting and then freeze its wait time counter (Kurose, 2007:534). In this scenario a collision is avoided if the competing nodes are able to sense each others signals. However, there is still the hidden terminal problem.

Recall that the hidden terminal problem occurs when two nodes can sense signals from the AP but are far enough apart that they cannot detect each other's signals. If a node cannot detect if the channel is busy, it will not be able to avoid collisions. To help solve the hidden terminal problem, the 802.11 standard has an optional reservation scheme that helps avoid collisions in this situation. In this reservation scheme, the Wi-Fi protocol has the transmitting wireless station or AP sends out a Request to Send (RTS) control frame to the receiving AP prior to transmitting any data. This RTS frame indicates the total time that the transmitting node requires to transmit the entire data frame and to subsequently receive the acknowledgement frame. The receiving AP, assuming the RTS frame was received, replies by broadcasting a Cleared to Send (CTS) frame. The CTS frame gives the sending node permission to send its data frame and also alerts any other nodes to not send data during the reserved time period. This RTS/CTS exchange process is typically only used to reserve the channel for the transmission of large data frames. Since the RTS/CTS exchange is optional, if it is being used, a wireless station or AP can set an RTS threshold size so that the RTS/CTS exchange only occurs when the frame is larger than the threshold size. Usually, a wireless station has the RTS threshold value set to be larger than the maximum frame size, which means that the RTS/CTS exchanged is omitted completely (Kurose, 2007:535-537). Now that the basic protocols used by 802.11 are defined, the next section will explain 802.11 security.

802.11 Security

In a closed data network, data is transmitted between nodes through a wired medium. In order for an outside party to be able to view or intercept data between nodes, the other party would need to be located in the wired medium between the two communicating nodes. In a wireless network, the medium is the free space radio channels between nodes. Unlike a wired medium, data frames transmitted via a wireless network can be viewed and intercepted by anyone capable of receiving the signal. For this reason a layer of security is required in order to encrypt data between nodes. There are many security techniques that can be implemented in the 802.11 standard. Explaining all of the different techniques that exist would require a separate dedicated paper. This project will discuss two of the most widely used 802.11 security schemes in small office and home networks; Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

The security standard that was initially defined in the IEEE 802.11 standard is known as WEP. The WEP security protocol provides authentication and encryption between wireless stations and the AP using a symmetric shared key method. In this protocol the AP and the wireless station need to agree on a 40-bit or 104-bit symmetric key using an out-of-band method, such as encrypted e-mail, standard post office mail, telephone call, etc. The following defines the basic steps in the WEP protocol during the authentication process.

1. A wireless station transmits an authentication frame to an AP.
2. The AP responds to the authentication frame with a 128-byte nonce value.
3. The wireless station then encrypts the nonce using the shared key and transmits back to the AP.
4. The AP then decrypts the encrypted nonce. If the nonce matches the original nonce sent by the AP then the wireless station is authenticated (Kurose, 2007:733).

The data encryption algorithm used in the above authentication process and for data encryption is described in the following list.

1. A 4-byte cyclical redundancy check (CRC) value is computed for the data payload.
2. The payload and the CRC are then encrypted using the RC4 cipher. The RC4 cipher is given a 64-bit key; the algorithm then produces a stream of key values that are used to encrypt the data and CRC value in the frame. The 64-bit key is the 40-bit symmetric key with a 24-bit Initialization Vector (IV) appended. The IV changes for each frame and is in plaintext in the header of each WEP encrypted frame.
3. The receiving node creates the 64-bit key using the shared 40-bit symmetric key and adding the 24-bit IV located in the header.

4. The receiving node then decrypts the frame using the 64-bit key (Kurose, 2007:733-734).

5. Since WEP was the first attempt at a wireless security standard, there are inherent flaws in the algorithm which make cracking the symmetric key feasible. These flaws and the techniques to exploit them will be discussed later in this project.

The IEEE solution to the weak security of 802.11 WEP is the 802.11i standard. As with all standards, issuance, ratification, and implementation by the users of the standard can take years. In order to bridge the gap between the weak security of the 802.11 WEP and the stronger security of 802.11i, WPA was implemented as an interim upgrade to existing 802.11 devices and also provides compatibility with the 802.11i standard. Table 2 shows a comparison of the WEP and WPA protocols.

Table 2. WEP vs. WPA comparison

	WEP	**WPA**
Encryption	Flawed, cracked	Fixes all WEP flaws
	40-bit & 104-bit keys	128-bit keys
	Static – same key used by everyone on the network	Dynamic session keys. Per user, per session, per packet keys
	Manual distribution of keys – hand typed into each device	Automatic distribution of keys
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication, utilizing 802.1X and Extensible Authentication Protocol (EAP)

One of the biggest differences between WEP and WPA is that WPA uses a larger 128-bit key. More importantly, WPA uses dynamic session keys, has a mechanism for automatically distributing the keys, and employs stronger authentication protocols. These WPA improvements, however, only exist in large networks where an authentication server is utilized. Small office and home users utilizing WPA still are required to use a pre-shared static key (PSK) that needs to be input into the AP and the wireless stations that communicate with the AP. The PSK and the SSID in the WPA protocol are used to compute the Pairwise Master Key (PMK). Using the PMK, rather than the PSK, these small network users obtain more security through the use of the WPA Temporal Key Integrity Protocol (TKIP).

TKIP is a collection of algorithms created to fix the security problems of WEP while also maintaining backward compatibility with older hardware. TKIP basically provides additional security by offering an additional protocol around WEP. The following list defines the elements of TKIP:

1. A Message Integrity Code (MIC) is a cryptographic checksum using the source and destination MAC addresses and the plaintext data of the 802.11 frame. The MIC protects against forgery attacks.
2. Countermeasures that bound the probability of successful forgery of data and the amount of information an attacker can learn about the key.
3. An extended 48-bit IV and an IV sequence counter, called the TKIP sequence counter (TSC), which addresses replay attacks.

4. Per packet key mixing of the IV is used to break up the correlation used by weak key attacks (Eaton, 2002).

As presented in the above list, TKIP uses a 48-bit IV called the TSC. By using a 48-bit TSC, as opposed to a 24-bit IV, the probability that an IV will be used more than once in a single association is almost zero. Since the TSC is updated for each packet, 2^{48} packets can be exchanged using a single temporal key before a key would need to be used again. Under heavy, steady internet traffic loads, the requirement to reuse a key would take approximately 100 years (Eaton, 2002).

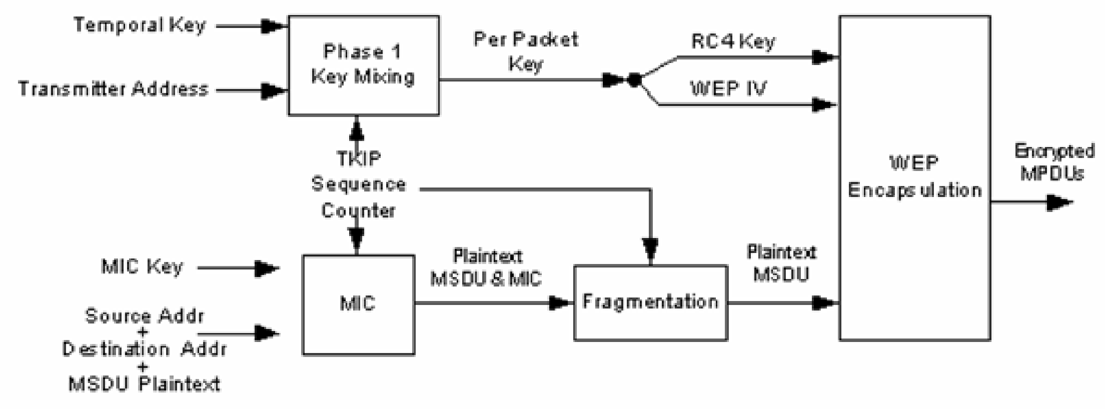


Figure 5. TKIP Encapsulation Process (Eaton, 2002)

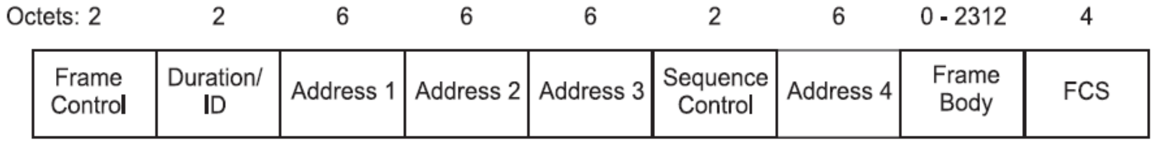
The TSC is constructed from the first and seconds bytes of the original WEP IV and 4 bytes provided in the extended IV. The TKIP encapsulation process is shown in Figure 5. The temporal and MIC keys are derived from the PMK. The temporal key, transmitter address and TSC are combined in a two-phase key mixing function to generate a per packet key to be used to seed the WEP engine for encryption. The per packet key is 128 bits long and is split into a 104-bit RC4 key and a 24-bit IV for presentation to the WEP engine. The MIC is calculated using the source MAC address, destination MAC address, the plaintext data of the 802.11 frame, the MIC key and the TSC. By computing the MIC using the source and destination MAC addresses, the data is keyed to the sender and the receiver which aids in preventing forgery attacks (Eaton, 2002).

The decryption process is basically the same as the encryption process with some exceptions. After the recovery of the TSC from the received frame, the TSC is compared to the previous frame received to see if the most recent frame has a greater value. If the received frame does not have a greater TSC value, the frame is discarded in order to prevent a replay attack. Also, the MIC value is recalculated at the receiving node and is compared to the decrypted MIC value retrieved from the received frame. If these values do not match, then countermeasures are taken, which primarily consists of rekeying the temporal key (Eaton, 2002).

As can be seen, the WPA algorithm provides for more security than WEP. However, much like WEP, the security of WPA using PSK is only as strong as the shared-key used by the AP and wireless stations. If this key becomes compromised, all security is lost and can only be regained by manually inputting new keys into the AP and wireless stations. Now that the basics of 802.11 security and encryption have been defined, the next step is to discuss the architecture of the actual 802.11 frame.

The 802.11 Frame

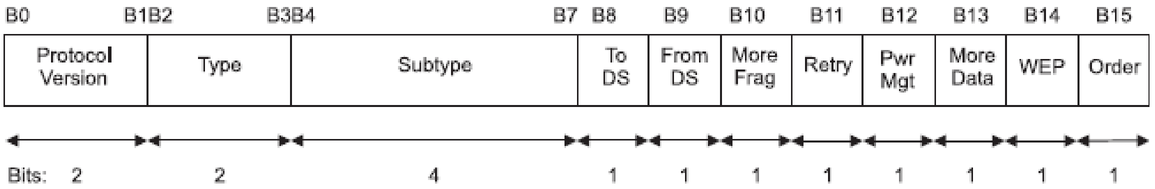
The standard 802.11 frame is shown in Figure 6. The numbers above the fields are the length of the field in bytes, while the numbers below the subfields in Figure 7 are the length in bits.



Octets: 2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

Figure 6. The 802.11 frame (IEEE, 1999:34)

The first part of the data frame is the control field and is shown in Figure 7. Some of the more important subfields in the control field are as follows:



B0 B1	B2 B3	B4 B7	B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order
Bits: 2	2	4	1	1	1	1	1	1	1	1

Figure 7. The Frame Control Field (IEEE, 1999:35)

Type and Subtype Subfields: used to distinguish the association, RTS, CTS, ACK, and data frames. Table 3 shows the values for some of the frames already discussed.

Table 3. Type and Subtype Combinations

Type Value	Subtype Value	Description
00	0000	Association Request
00	0001	Association Response
01	1011	RTS
01	1100	CTS
01	1101	ACK
10	0000	Data

To/From Subfields: Used to define the meanings of the different address fields. These meanings change on whether ad hoc or infrastructure modes are used. In infrastructure mode these fields define whether an AP or wireless station is sending the frame (Kurose, 2007:541). Table 4 shows the different to/from combinations and their meanings.

Table 4. To/From Subfield Combinations

To Value	From Value	Description
0	0	Ad hoc: data frame sent from one wireless station to another wireless station
1	0	Infrastructure: data frame to the AP from a wireless station
0	1	Infrastructure: data frame from the AP to a wireless station
1	1	Infrastructure: data frame from one AP to another AP

Wired Equivalent Privacy (WEP) Subfield: When set to 1, this subfield indicates that the data has been processed through the WEP algorithm and the entire frame format is expanded (IEEE, 1999:37). WEP will be discussed further in the 802.11 security section.

After the frame control field, the other fields of the 802.11 frame header continue. The more important fields are as follows:

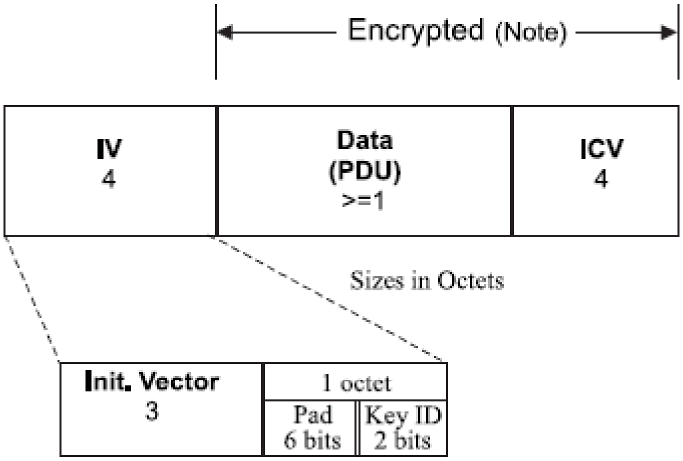
Address 1 Field: This is the MAC address of the wireless station that is to receive the frame. If a wireless station is transmitting to an AP, the AP MAC address would be in address 1.

Address 2 Field: This is the MAC address of the wireless station that transmitted the frame. If a wireless station is transmitting to an AP, the MAC address of the wireless station would be in address 2.

Frame Body Field: This field contains the payload of the frame, typically an IP datagram or an ARP packet. Although the payload can be as large as 2312 bytes, it is usually less than 1500 bytes.

Frame Check Sequence (FCS) Field: The FCS, also known as the CRC, is used by the receiver to detect bit errors in the received frame and is computed over the entire data frame.

The 802.11 frame explained in the previous section is the construction that can be expected for unencrypted data frames. When WEP or WPA security protocols are utilized there are some changes that occur to the assembly of the data frame. When using the WEP protocol for encryption, changes occur to the frame body. As explained previously in the WEP protocol, a 64-bit key is used to encrypt the original frame body data and CRC value. This 64-bit key is comprised of a 24-bit IV and a 40-bit or 104-bit pre-shared key. After the data and CRC are encrypted they are placed inside the frame body and appended with the 24-bit IV that was used during the encryption process.



NOTE – The encypherment process has expanded the original Frame Body by 8 octets, 4 for the IV field and 4 for the ICV. The ICV is calculated on the data field only.

Figure 8. Construction of Expanded WEP Frame Body (IEEE, 1999:64)

Figure 8 shows how the WEP protocol changes the frame body of the 802.11 data frame. As the note below the Figure 8 explains, the frame body transmitted when using the WEP protocol for encryption expands the original frame body data by 8 bytes (octets). 4 bytes are for the IV field and the other 4 are for the WEP integrity check value (ICV), another CRC. The WEP ICV value is calculated using the original frame body data and is encrypted with the data where as the FCS field is calculated using the entire frame. The 4-byte IV field is composed of three subfields. The first 3 bytes are the 24-bit IV that was used in the 64-bit key to encrypt the data.   The last byte of the IV field contains a 6-bit pad followed by a 2-bit Key ID field. The Key ID field identifies 1 of 4 possible pre-shared key values to use in decrypting the frame body (IEEE, 1999:64-65).

When the WPA protocol is utilized, changes occur to the frame body as well. As explained previously, the TKIP protocol used in WPA uses an extended 48-bit IV called the TSC. Also, TKIP uses a MIC function that creates the 8-byte MIC value using the source MAC address, destination MAC address, the plaintext data of the 802.11 frame, the MIC key and the TSC. The assembly of the frame body when using WPA with TKIP is shown in Figure 9.

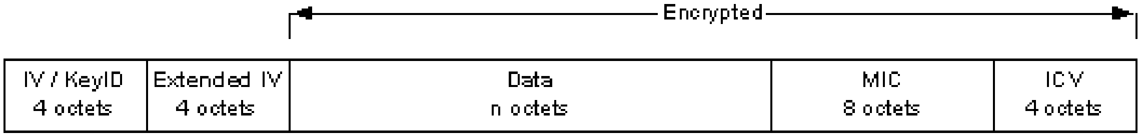


Figure 9. Frame Body After TKIP encryption (Eaton, 2002)

When compared to the WEP encrypted 802.11 frame body, the WPA frame body increases the frame body by 12-bytes. The first 4 of these bytes are the extended IV which is used in conjunction with the first 2 bytes of the original WEP IV to create the

48-bit TSC. The other 8 bytes are the MIC value that is encrypted along with the original frame body content and the WEP ICV. By using WPA encryption, the total increase of the frame body from the unencrypted frame is 20-bytes (Eaton, 2002).

III. Attacking the Wi-Fi Protocol

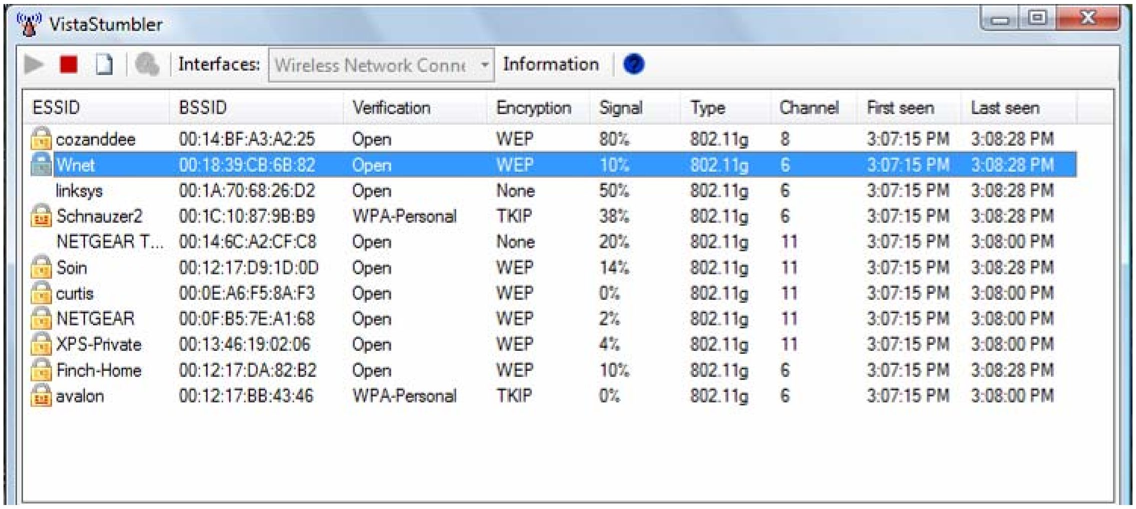
Now that the fundamentals of the 802.11 protocol have been explained, steps will be discussed to defeat a wireless station or AP that is utilizing the Wi-Fi protocol. This concept of operations will be broken down into three sections; detection, denial, and deception. The first section will analyze the protocol and discuss techniques that can be used to detect wireless networks that are located near a location and to then determine the AP a wireless station is utilizing. The next two sections will discuss how to defeat an 802.11 signal once the network has been detected. The first technique for defeating an 802.11 wireless network will analyze techniques for denying the use of the network. Denial can be achieved either through broad area denial in which no one can utilize the network, or through specific network denial, which would deny only a limited number of users from utilizing the network. The second technique for defeating an 802.11 wireless network will discuss techniques that can be used to deceive the signals transmitted to or received from the wireless station. The techniques that will be derived in the following section are theoretical with no actual application. When available, tools that are currently available to apply these techniques will be briefly presented.

Detecting Unauthorized Channels

The first step in defeating a wireless station or AP that is utilizing the 802.11 protocol is to detect the wireless network that is being used. The majority of commercially available equipment on the market today (2008) utilizes either the 802.11b or 802.11g standards, with 802.11g being the newer and faster of the standards. Both of these standards operate in the 2.4-2.485 GHz range and operate on 1 of 11 overlapping channels. Since there are only 11 possible channels that an 802.11 wireless station or AP can operate on, the ability to detect Wi-Fi wireless signals becomes simpler. However, detecting a specific wireless network can still be daunting when there are dozens of other wireless networks in the same vicinity. One solution is to procedurally control and restrict the 802.11 channels that can be used at a specific location to one or two channels. If a wireless network appears that is utilizing a restricted channel, that wireless network and channel can be denied without affecting legitimate users. However, if a wireless network utilizes one of the allowable channels, denying the channel would affect legitimate users. Detecting the channel that the wireless network is utilizing is only part of solving the puzzle. In order to determine a specific wireless network, the SSID of the network needs to be detected. There are two major categories for detecting 802.11 networks; active and passive.

Actively Detecting SSIDs

When actively scanning for Wi-Fi wireless networks, a wireless station broadcasts probe request frames. The APs that are within range of the wireless station receive the probe request frame and respond with a probe response frame. The wireless station then decides which responding AP to associate with. This probe request frame can also be used to search for a network with a specific SSID. Tools that use active scanning to detect Wi-Fi networks periodically send out these probe response frames (Cache, 2007:92). Windows based tools that use active scanning are NetStumbler (Windows XP and earlier) and VistaStumbler (for Windows Vista). Figure 10 shows a screen shot of VistaStumbler. From the screen shot it can be seen that VistaStumbler gathers the MAC address, SSID, wireless channel and relative signal strength of each AP that responds to the probe request frame (Skoudis, 2006:243). Also, if any encryption is used, the



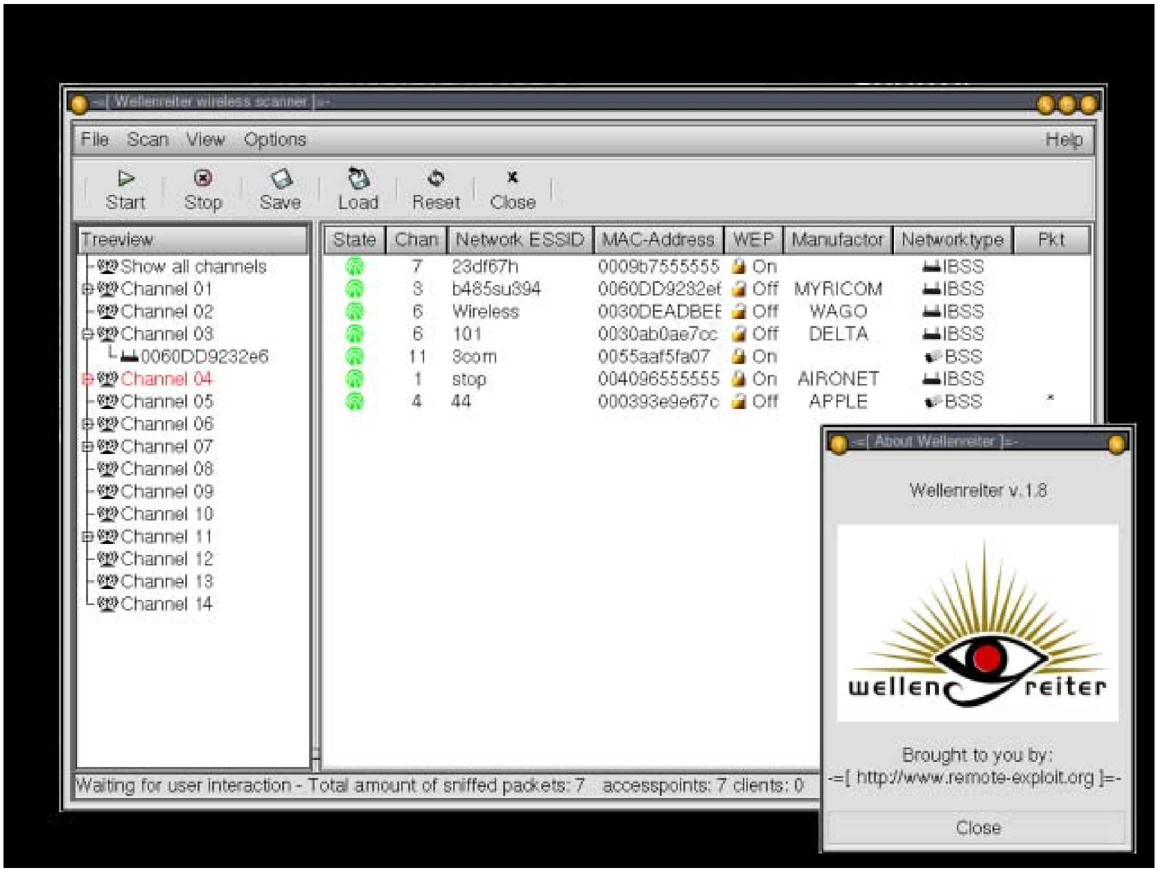
ESSID	BSSID	Verification	Encryption	Signal	Type	Channel	First seen	Last seen
cozanddee	00:14:BF:A3:A2:25	Open	WEP	80%	802.11g	8	3:07:15 PM	3:08:28 PM
Wnet	00:18:39:CB:6B:82	Open	WEP	10%	802.11g	6	3:07:15 PM	3:08:28 PM
linksys	00:1A:70:68:26:D2	Open	None	50%	802.11g	6	3:07:15 PM	3:08:28 PM
Schnauzer2	00:1C:10:87:9B:B9	WPA-Personal	TKIP	38%	802.11g	6	3:07:15 PM	3:08:28 PM
NETGEAR T...	00:14:6C:A2:CF:C8	Open	None	20%	802.11g	11	3:07:15 PM	3:08:00 PM
Soin	00:12:17:D9:1D:0D	Open	WEP	14%	802.11g	11	3:07:15 PM	3:08:28 PM
curtis	00:0E:A6:F5:8A:F3	Open	WEP	0%	802.11g	11	3:07:15 PM	3:08:00 PM
NETGEAR	00:0F:B5:7E:A1:68	Open	WEP	2%	802.11g	11	3:07:15 PM	3:08:00 PM
XPS-Private	00:13:46:19:02:06	Open	WEP	4%	802.11g	11	3:07:15 PM	3:08:00 PM
Finch-Home	00:12:17:DA:82:B2	Open	WEP	10%	802.11g	6	3:07:15 PM	3:08:28 PM
avalon	00:12:17:BB:43:46	WPA-Personal	TKIP	0%	802.11g	6	3:07:15 PM	3:08:00 PM

Figure 10. VistaStumbler

protocol is displayed. Although an active scanner can detect many Wi-Fi networks, the tool can only detect probe response frames from those APs that are configured to respond to probe request frames. These active scanners are unable to detect APs that do not respond to broadcast probe request frames or any other Wi-Fi traffic.

Passively Detecting SSIDs

To detect these other APs or any other wireless traffic, passive scanning tools are used. These tools typically generate better results than active scanning tools. These tools do not transmit any packets themselves but rather listen to all packets and then analyze the packets to detect wireless networks. These tools require that a wireless network card be placed into monitor mode, which is similar to placing an Ethernet card into promiscuous mode. This sounds simple enough, however, not all wireless cards support monitor mode. A card that does support monitor mode simply listens to all the frames that it can detect, analyzes the frames, and then updates the user interface as new information is determined (Cache, 2007:95-96). There are currently no passive scanning tooling tools that are Windows based. However, two Linux based passive scanning tools that work with monitor mode capable wireless cards are Wellenreiter and Kismet. These tools can detect a wireless network that is not broadcasting an SSID with its probe response frame by listening to traffic on the network. If traffic is idle on the wireless network, these tools can detect the network based on the MAC address of the AP, but cannot determine the SSID until some traffic is generated on the network. Figure 11 shows a screenshot of Wellenreiter. As can be seen from the screenshot, Wellenreiter displays the channel, SSID, MAC address, and if WEP encryption is used or not. The only disadvantage these passive tools have when compared to the active scanners is that any encryption level above WEP is not identified.



State	Chan	Network ESSID	MAC-Address	WEP	Manufactor	Networktype	Pkt
●	7	23df67h	0009b7555555	On		IBSS	
●	3	b485su394	0060DD9232et	Off	MYRICOM	IBSS	
●	6	Wireless	0030DEADBEE	Off	WAGO	IBSS	
●	6	101	0030ab0ae7cc	Off	DELTA	IBSS	
●	11	3com	0055aaf5fa07	On		BSS	
●	1	stop	004096555555	On	AIRONET	IBSS	
●	4	44	000393e9e67c	Off	APPLE	BSS	*

Waiting for user interaction - Total amount of sniffed packets: 7 accesspoints: 7 clients: 0

Wellenreiter v.1.8

Brought to you by:
-=[http://www.remote-exploit.org]=-

Figure 11. Wellenreiter (freshmeat.net, no date)

Active and Passive Detection Combination

Using passive and active scanning tools, nearly all of the wireless networks near a location can be detected. The only Wi-Fi networks that cannot be detected are those that do not broadcast their SSID in the probe response frames, do not respond to broadcast probe request frames, and have idle or very minimal traffic. As stated earlier, almost all information from these wireless networks, except the SSID, can be determined through passive scanning tools. One method of determining the SSID is to wait for traffic to be generated on the desired network. Another technique for determining an idle network SSID is by forcing deauthentication.

In order for this technique to work, the MAC address of the desired non-broadcasting wireless network needs to be known. This information, as shown previously, can be obtained using one of the passive scanning tools. Spoofing the MAC address of the AP, a deauthenticate message is sent to the broadcast address of the wireless network. The deauthenitcate message is a type of control message and is therefore accepted by any wireless stations currently on the network without authentication. The result of this message being sent is that any wireless stations currently associated with the spoofed AP are disassociated with the network. After the wireless stations are disassociated, they will automatically try to reassociate with the AP using the required SSID. These association frames contain the SSID in clear text and can now be detected by one of the passive scanning tools. By forcing deauthentication, this technique is essentially injecting traffic into the desired wireless network (Skoudis, 2006:247). One tool that is commercially available that performs this technique is a Linux based tool called Airjack. By using this tool, in conjunction with an active and passive scanning tool, all 802.11 wireless networks can be detected. After the desired network has been detected, the next step is to defeat the wireless network.

Defeat through Denial

The first course of action that can be taken to defeat a desired wireless network is through Denial of Service (DoS). There are two types of DoS that can be performed. The first type will be called broad area denial. Broad area denial techniques affect not only the desired wireless network but also legitimate wireless networks in the vicinity of the desired wireless network. The second type of DoS will be called specific network denial. Specific network DoS techniques affect only the desired network.

Broad Area Denial

Noise Jamming

One of the simplest forms of broad area denial techniques is noise jamming which is an active jamming technique. First, a wireless network is detected and the 802.11 channel of the network is determined. An RF jamming source can be utilized to send out a powerful signal on the same frequency of the desired network. This signal contains no information but only noise. The jamming signal denies the use of the frequency since actual signals in the frequency will be lost in the background noise generated by the jamming source. The first disadvantage of performing this type of DoS is that the frequency being jammed becomes unusable by all wireless networks, not just the desired network. The second disadvantage of this technique is that active noise jamming is typically not effective against wireless networks incorporating spread spectrum and multiplexing technologies. A discussion of these technologies is beyond the scope of this project however all that needs to be known is that these technologies are used in 802.11

wireless networks and one of their main goals is to minimize interference (noise) from external sources and other network users.

Cleared to Send Control Frames

Another broad area DoS technique involves utilizing the 802.11 infrastructure and protocols. Recall that 802.11 networks have to deal with a dilemma called the hidden terminal problem. This problem occurs when two wireless stations are connected to an AP and they are unable to receive each other's signals. Since the wireless stations cannot detect each other, one station is unable to detect when the other station is transmitting. The portion of the 802.11 protocol that deals with this problem uses RTS and CTS control frames. An RTS frame is sent by the wireless station desiring to send information and the CTS frame is broadcast by the AP to tell other wireless stations not to transmit during a specified time frame. There are two techniques that this portion of the protocol can be manipulated in order to perform DoS on a desired network. The first technique is to generate an RTS frame and transmit the frame to the AP of the rogue wireless network. The AP will receive this RTS and then broadcast a CTS frame to every wireless station in the vicinity of the desired AP, not just the wireless stations associated with the AP. The second technique is to self generate and transmit a CTS frame by spoofing the MAC address of the desired AP. One advantage of creating and transmitting the CTS frame is that a continuous stream of CTS frames are transmitted that can bring the throughput of the network down to almost zero. Another advantage of this technique is that the location of the AP is not required (Cache, 2007:195). As with active noise jamming, the disadvantage of RTS/CTS spoofing is that it affects all wireless stations within the vicinity of the desired network, denying legitimate users wireless network access. As can be seen, these techniques are good at denying a wireless network from operating but poor at limiting the effects to a single network.

Specific Network Denial

In order to have a DoS effect on a specific network, one needs to become associated with the network. Associating with an unsecured wireless network is quite simple since the SSID and MAC address of the AP are all that are required to either associate with the AP or to create a fake AP. When encryption is used the process increases in difficulty since the keys used by the encrypted network need to be cracked. Once the keys are cracked, associating with a rogue network becomes is simplified.

Associating with a WEP Secured Network

Recall that the basic encryption scheme that is utilized in the 802.11 protocol is WEP. The inherent flaw with WEP is how the IVs are used in each encrypted data frame. When the WEP protocol is used, the 24-bit IV is added to the 40-bit or 104-bit pre-shared secret key and then the RC4 algorithm is used for encryption. When the encrypted frame is transmitted the IV is located before the encrypted data in the frame body in clear text. This means that the first 3 bytes of the key are transmitted in the clear and viewable by anyone who can intercept the data frames (Cache, 2007:180). When properly utilized, the RC4 algorithm requires that the same 64-bit key value never be reused. With WEP, the IV is only 24-bits long, which translates into only 2^{24} unique keys that can be used. If the IVs are chosen randomly the probability of having chosen the same IV value is more than 99 percent after only 12,000 frames. If a node is transmitting 1 kilobyte frames at a transmission rate of 1 Mbps, the node will have transmitted 12,000 frames within a few seconds. Anyone viewing the transmitted frames can easily determine when a duplicate IV occurs (Kurose, 2007:734). This type of WEP key cracking is called a statistical attack. In order to quickly break a WEP key around 300,000 frames would be required for a 40-bit key, and almost 1,000,000 frames for a 104-bit key. When a network is idle or has very sparse traffic, more traffic can be generated by retransmitting intercepted frames back into the wireless network. Frames that contain address resolution protocol (ARP) requests and responses are optimal for generating more network traffic because these frames are of a uniform and unique size. If there are very few nodes on a network, the content of frames containing ARP packets can be more easily deciphered since some of the encrypted content is already known, such as the sending and receiving MAC addresses.

There are numerous commercially available tools that can decipher WEP keys, but one of the most popular tools is Aircrack. This tool is available on Linux and Windows based systems, but operates best on Linux based systems (Cache, 2007:181). Other tools that can assist Aircrack in decrypting WEP keys are Aireplay and Airodump. Aireplay is another Linux based tool that is used to inject frames into the network to generate more frames which are then captured using Airodump and placed into a capture file. Aircrack then performs the statistical analysis attack on the captured frames to statistically determine the WEP key. Once the WEP key has been cracked the desired network can now be associated with. Now that the techniques for cracking a WEP key have been shown, the next problem is dealing with a wireless network that uses WPA encryption.

Associating with a WPA Secured Network

Recall that WPA encryption is stronger than the encryption used in WEP. However, much like cracking a WEP key, a WPA key can be determined by capturing certain frames from the desired WPA encrypted network. These specific frames are transmitted during the WPA authentication process. Figure 12 shows the steps of a successful four-way handshake with an AP utilizing WPA encryption. In the first part of the authentication process the client and the AP use the PSK and the SSID of the network to compute the PMK. Using the PMK, the client (wireless station) communicates with the AP using a protocol to create a new Pairwise Transient Key (PTK). The PTK is created dynamically every time the client connects to the AP and can change during a connection. The PTK is created through a function using the PMK, the A-nonce (an AP produced random number), the S-nonce (a client produced random number), the client

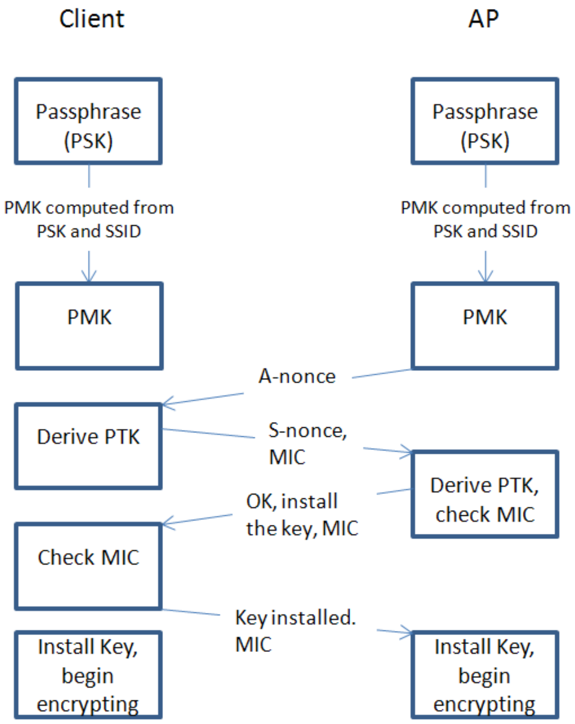


Figure 12. WPA 4-way Handshake

MAC address, and the AP MAC address. The AP verifies that the client has the correct PMK by checking the MIC value during the authentication process. The client also verifies that the AP has the correct PMK using the MIC value. The numbers that are required when cracking a WPA PSK are the A-nonce, S-nonce, and the MIC value. Once these numbers are captured, in addition to the SSID, cracking of the PSK can commence. Unlike cracking WEP, there is no statistical attack on WPA keys (Cache, 2007:205-206). To crack a WPA PSK a dictionary attack is utilized. A dictionary attack is a brute force attack that uses a list of words that are fed one at a time into the WPA authentication algorithm used to create the MIC value. If the calculated MIC value matches the captured MIC value then the tested word is the PSK. A dictionary attack is guaranteed successful in cracking the PSK. However, depending on the complexity of the passphrase, the process can take an extraordinarily long time to complete.

One tool that is used to crack a WPA PSK is coWPAtty (correct spelling). Cowpatty is a Linux based tool that performs the dictionary attack on the PSK once the required information is captured. This tool processes approximately 30-60 words per second, which appear to be relatively fast. Processing 45 words per second tests 3,888,000 words per day. This number seems large, but there are 208,827,064,576 possible ways to create an 8-character WPA passphrase. At this rate cowpatty would take 53,710 days to test all possible 8-character WPA passphrases (Fogie, 2005). This time can be shortened either by using a hardware accelerated version of Cowpatty, pre-creating hash tables using popular SSIDs (such as Linksys), or by using multiple computers, each processing a different portion of the dictionary word list. Despite the possibility of a lengthy computational period, a WPA PSK dictionary attack can crack the

PSK quickly, considering the propensity of wireless network users to choose weak passwords to encrypt their networks. After the passphrases and keys for a WEP or WPA encrypted wireless network are obtained, the ability to prosecute a DoS against a specific wireless network can occur.

Creating a Fake AP

As stated earlier, a DoS attack against a specific wireless network starts by associating with the desired network. This requires the SSID of the network and the WEP/WPA keys, if required. Using this information and then transmitting a stronger signal than the AP of the desired wireless network, a fake AP can be created. The first step of this process is to transmit a deauthentication control message. Recall that this message disassociates all wireless stations from the network. When these wireless stations attempt to re-associate with the AP, they will automatically connect to the fake AP. Then the frames that are intercepted are simply discarded. As long as the fake AP behaves like the actual AP, the wireless stations will assume that their transmitted frames were received and forwarded. This technique can be effective against a majority of the wireless stations associated with a network by using an omnidirectional antenna. This same technique can be performed against a single wireless station by utilizing a directional antenna. Using either type of antenna, the result of this technique is that only the desired wireless network is affected. Users on other wireless networks are able to continue operating normally.

Defeat through Deception

The last section discussed techniques for defeating a desired wireless network through denial. Some denial techniques can be noisy and alert the operator of a wireless network that the network is operating incorrectly allowing the operator to reconfigure the system to avoid the DoS. In some instances denial may be the only avenue for defeating a wireless network, such as heavily secured networks. Another course of action is to defeat the network through deception. When deceiving a wireless network, the network seems to operate normally while the information being sent across the network is being altered.

ARP Spoofing

As in applying denial techniques, the first step in deceiving a desired wireless network is to associate with the network. The same techniques of WEP/WPA key cracking that were presented in the previous section are also applied here. Once associated with the desired network a technique called ARP spoofing is utilized. ARP packets are used in a network to determine the MAC address of a receiving node. A node that has a frame to transmit sends out an ARP query. An ARP query is broadcast to every node on the network to determine which node on the network has a specific IP address. When receiving an ARP query, a node determines if it has the requested IP address. If the node has the desired IP address, an ARP response is transmitted back to the requesting node which providing the MAC address of the requested IP address. The requesting node now knows where to transmit the frame. If the receiving node does not have the desired IP address then the node does nothing and the query is ignored (Kurose, 2007:465-467).

After associating with the desired network, the first step in ARP spoofing is to determine the AP IP and MAC addresses and the desired wireless station IP and MAC addresses. These are determined by analyzing intercepted packets from the network. The next step is to transmit gratuitous ARP reply messages into the network. One of the ARP reply messages is transmitted to the AP stating that the IP address of the wireless station is located at the MAC address of the spoofing wireless station. The other ARP reply message is transmitted to the wireless station. This message states that the IP address of the AP is located at the MAC address of the spoofing wireless station. These reply messages are continually transmitted to ensure that the AP and wireless station keep mapping the other's IP address to the spoofing wireless station. Now, when either the AP or the wireless station transmits a frame, the frame will be transmitted to and received by the spoofing wireless station. The spoofing wireless station can then intercept all of the frames to and from the desired wireless station and then forward the frames to the correct locations. ARP spoofing has a minimal effect on the operation of the network creating the perception that the network is operating normally.

Altering Packet Data

When ARP spoofing is utilized, intercepted frames are not only able to be viewed and analyzed by a third party, but the data inside the frames can be altered as well. Recall that the payload of an 802.11 frame is typically an IP datagram or an ARP packet. An IP datagram carries a payload of data which is typically a transport-layer segment. The transport-layer segment uses one of two transport protocols, TCP or UDP. These transport-layer segments contain the application layer messages. Application layer messages contain the data that two applications send to each other to communicate, such as e-mail, web site content, and video streams. This application layer message is the data that can be changed and manipulated.

With ARP spoofing, the process of manipulating data within a data frame has three general steps. First, the intercepted frame is un-encapsulated. This step is synonymous to peeling away the layers of an onion to get to the application message. The layers of the “onion” surrounding the application message are the 802.11 data frame, the IP datagram, and the TCP/UDP segment. These layers are preserved for later use. The second step changes or manipulates the application layer message.   For example, streaming video data can be deleted and replaced by alternate video data or e-mail text can be changed or replaced. The final step is to then re-wrap the application layer message with the preserved “onion” layers and then transmitted the frame to correct location. Ideally, the host receiving the application message is unaware that the data is being manipulated.

This process has been greatly simplified and in reality is a relatively difficult task. First, the entire process needs to occur quickly to avoid excessive end to end delays. Next, although the layers of the “onion” are preserved, some of the fields in each of the data frame, IP datagram and transport-layer segment headers will need to be recalculated such as the CRC values. Assuming this portion of the process can be performed quickly, the linch-pin of the entire process is the ability to insert the correct format of the application message. This format could be ascertained in real-time by first analyzing the intercepted packets and then subsequently manipulating the application message. If this entire process creates excessive delays or if the application message format cannot be determined, the deception of the network can revert to a DoS technique by discarding the captured packets. When utilized in this manner, ARP spoofing has the same effect as creating a fake AP.

IV. Summary

The purpose of this project was to present techniques for defeating 802.11 wireless networks. The initial section discussed some of the portions of the 802.11 protocol. After discussing the protocol, techniques to defeat an 802.11 wireless network were presented. The first step in defeating a network is to detect the network. Once the desired wireless network is detected, the process of defeating the network can begin. Defeating a wireless network was broken down into two sub-categories; denial and deception. Denying a Wi-Fi network was further divided into two types of denial; broad area denial and specific network denial. Broad area denial techniques included RF jamming and utilizing the RTS/CTS 802.11 protocol. These techniques did not require an association with the desired network. Specific network denial techniques however, do require an association with the desired network. Association with a network could be trivial if no security measures are utilized and increases in difficulty with the implementation of WEP and WPA security. Cracking of the WEP and WPA keys required to associate with a network may be time intensive requiring a broad area denial technique to defeat the network. After denial techniques were discussed, a process for defeating a wireless network using deception was presented. This deception process was actually a manipulation of the data encapsulated within the 802.11 frame rather than deceiving the actual signal.

The procedures presented in this project for detecting and defeating 802.11 wireless networks can be applied to the original motivation of this project; defeating 802.11 signals used to control UAVs. There are a number of tasks that need to be completed before these techniques can be transformed into a concise concept of operations. First, equipment for the task needs to be researched and purchased. This equipment ranges from computers to antenna types. In conjunction with this task, the various tools available that perform the presented techniques need to be analyzed and tested for functionality and compatibility with the equipment. Lastly, although many tools exist that perform the techniques defined in this project there are some techniques which require the development of tools that also need to be tested for functionality and compatibility.

This project was by no means an exhaustive presentation of defeating 802.11 wireless networks. The background of the threat, the 802.11 protocol and the techniques presented provide additional topics to research. WiMAX, 3G and 4G cellular data networks, and 802.11n are some examples of emerging wireless technologies that could be utilized to communicate with a UAV. As these network technologies become more widely proliferated the ability to purchase COTS parts becomes easier. Also, other portions of the 802.11 protocol could be used to create denial effects, such as malformed frames, turning on and off bits in the frame control field, and manipulating the 802.11 power management advanced feature. As with any technology, once techniques are developed that deal with a certain network or protocol, most likely a newer protocol or network is being developed which will require new research.

Bibliography

Air Force Research Laboratory and Aeronautical Systems Center. (2005). *Black dart III Air force Research Laboratory and Aeronautical Systems Center Team Final Report (draft).* Wright-Patterson Air Force Base, Ohio.

Cache, J., & Liu, V. (2007). *Hacking exposed: Wireless*. New York, New York: McGraw-Hill.

Eaton, D. (2002). *Diving into the 802.11i spec: A tutorial.* Retrieved 4/28, 2008, from http://www.commsdesign.com/showArticle.jhtml?articleID=16506047

Freshmeat.com. (2008). *Screenshot of project wellenreiter.* Retrieved 4/29, 2008, from http://freshmeat.net/screenshots/17961/

Grabinowski, E., & Brain, M. *How WiMAX works.* Retrieved 3/21/2008, 2008, from http://computer.howstuffworks.com/wimax.htm/printable

IEEE. (1999). *Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*. New York, New York: The Institute of Electrical and Electronics Engineers.

Keeney, F. *DEFCON WiFi shootout 2005 video.* Retrieved 03/21, 2008, from http://pasadena.net/shootout05/

Kurose, J. F., & Ross, K. W. (2007). *Computer networking: A top-down approach* (4th ed.). Boston, Massachusetts: Addison Wesley.

Merritt, A. D. (2005, 07/26/2005). Free wireless network up and running in olney. [Electronic version]. *Philadelphia Business Journal.*

Skoudis, E., & Liston, T. (2006). *Counter hack reloaded*. Upper Saddle River, New Jersey: Prentice Hall.

Wi-Fi Alliance. (2003). *Wi-fi protected access: Strong, standards-based, interoperable security for today's wi-fi networks.* Unpublished manuscript.

Vita

Major Charles R. Cosnowski was born in Southfield, Michigan and was commissioned a second lieutenant in the United States Air Force after graduating from the United States Air Force Academy in 1995 with a degree in Astronautical Engineering. He is a United States Air Force Weapons School graduate/instructor and fighter pilot with over 1400 hours in the F-16C, F-117A and T-38A. Major Cosnowski also holds two masters degrees; a Master of Science in Aerospace Engineering from the University of Colorado and a Master of Aeronautical Science in Aeronautics Specialization and Aviation Management from the Embry-Riddle Aeronautical University. He is currently attending the Air Force Institute of Technology graduating in June 2008 with a Master of Cyber Warfare.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)* 01-06-2008	**2. REPORT TYPE** **Master's Graduate Research Project**	**3. DATES COVERED** *(From – To)* Jun 2007 – Jun 2008

4. TITLE AND SUBTITLE Defeating 802.11 Wireless Networks	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Cosnowski, Charles R., Major, USAF	**5d. PROJECT NUMBER** If funded, enter ENR #
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/ICW/ENG/08-01
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Homeland security of the United States is constantly under threat of attack from terrorist organizations. A viable and current terrorist threat is the use of unmanned aerial vehicles (UAVs) as weapons of mass destruction. These UAVs can be built simply and cheaply from commercial off the shelf (COTS) parts and are typically controlled using standard radio control (RC) technology. An emerging technology that is being implemented to control and communicate with UAVs is the 802.11 wireless network protocol or Wi-Fi.

This project discusses various portions of the Wi-Fi protocol and analyzes the protocol to determine techniques for first detecting and then defeating wireless networks utilizing the protocol through denial or deception. The first set of techniques presented defeats a network through denial. These denial techniques are divided into two categories: broad area denial techniques and specific network denial techniques. After denial techniques are discussed a process for deceiving an 802.11 wireless network is presented.

15. SUBJECT TERMS
Wireless Computer Network, Local Area Networks, LAN, Data Links

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Robert F. Mills, PhD, USAF (ENG)
REPORT U	**ABSTRACT** U	**c. THIS PAGE** U	UU	56	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 4527: Robert.Mills@afit.edu